REMARKS

Claims 1-6, 8-16, 18-28, 30-41, 43-47 and 49-51 remain in this application. Claims 7, 17, 23, 29, 42, 48 and 52 have been previously cancelled. Claims 1, 6, 11, 16, 21, 28, 35, 41, 49, 50 and 51 have been amended. Claims 8, 18, 30, and 43 have been previously presented.

Applicant thanks the Examiner for the detailed study of the application and prior art.

Applicant notes the rejection of claims under 35 U.S.C. §101 as directed to non-statutory subject matter. Applicant thanks the Examiner for the explanation for the rejection that the claims recite "a mobile office platform server" but addresses the objection because, according to the Examiner, a server is not explicitly drawn to a machine and a server can encompass a server process, which is software alone. Thus, the claim does not recite any physical part of a device and does not fall into the statutory category of a machine.

Applicant has specifically amended each of the independent claims to recite the mobile office platform device. This device includes a database and as clearly set forth in paragraphs 35-40, the device may include in one example embodiment appropriate circuitry for running software programs such as SOAP and implement Active X controls and distributed objects and appropriate processing through an inherent processor

circuit that operates the various programs in conjunction with the database for storing data.

Thus, the claims as presented in this Amendment are explicitly directed to statutory subject matter.

Also, each of claims 6, 16, 28, and 41 are amended to delete the word "network" for consistency with the base claim.

Applicant also thanks the Examiner for the indication of allowable subject matter directed to claims 11-16, 18-20, 34-41 and 43-47, which include the independent claims 11 and 35.

The other independent claims have been amended to recite the plurality of connection engines distributed among a plurality of subnets and configured to access a server on an IP network (claims 1, 49, 50 and 51) or distributing connection engines over multiple subnets (independent claim 21). The independent claims as noted above have also been amended to recite the problem magnitudes and the preset rate of decay.

For the Examiner's reference, FIG. 1 of the instant application is reproduced below:

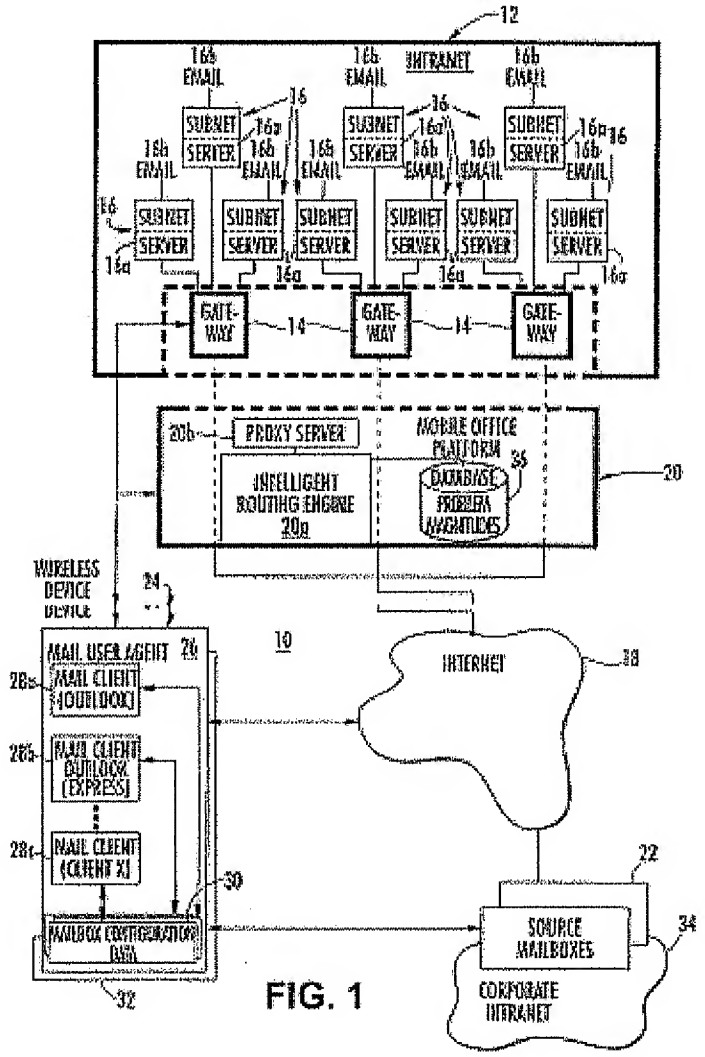


FIG. 1

The claimed communications system and method overcomes the technical drawbacks associated when a client such as operating from a personal computer at home, in a local area network or from a mobile wireless communications device, often attempts access to a server on the internet such as a website or email server, but fails to connect to the server and initiate the communications session. After repeated failures, a user may wait

a period of time and try again and possibly make a successful connection or fail to make a connection. The server could be actively blocking a connection request and this server may actively block or throttle connection requests based upon the originating IP address.

The claimed system and method distinguishes between a permanent or persistent transient failure in accessing the server and an intermittent or transient failure caused by other reasons. Thus, it overcomes the technical problems when temporary network outages occur on the internet and "failed" access attempts are retried. It aids to discern when certain servers may actively block a connection request.

As now claimed and as set forth in FIG. 1, a plurality of connection engines are distributed among a plurality of subnets and configured to access a server on an IP network. A mobile office platform device 20 includes a database for storing problem magnitudes relating to failed attempts at accessing servers using the connection engines and problem magnitudes and a preset rate of decay. The mobile office platform device includes an intelligent routing engine operative with the database for querying the database and delaying any further attempts at accessing the server when the problem magnitude as a preset rate of decay exceeds a predetermined threshold. A problem magnitude is assigned for an error based on failures unrelated to a network failure.

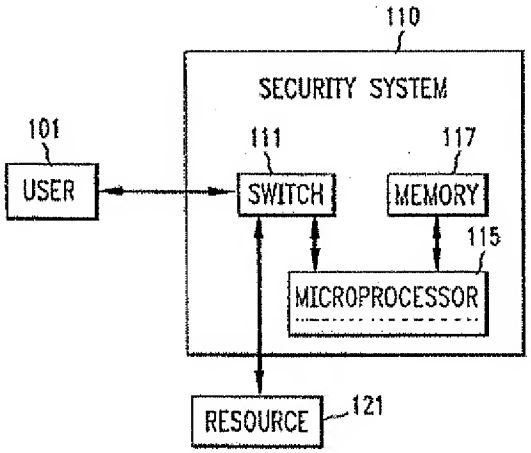
The dependent claims stress various features including the delaying of any reattempts at accessing a server until a problem magnitude returns to below a predetermined threshold and as a function of a preset rate of decay of a problem magnitude. In one aspect, the database includes data relating to a current problem magnitude for a failed access to a server that is added to a current exponentially decayed entry in the database. The database in another example includes data related to a problem magnitude versus time for any server in the connection engine pair. The failures unrelated to a network failure include an incorrect password and/or poorly formed request in one example.

The Examiner has rejected claims as anticipated by U.S. Patent No. 5,559,505 to McNair and other claims as obvious over McNair in view of U.S. Patent No. 7,251,065 to Bond et al. (hereinafter "Bond") or McNair in view of the previously cited Fodor. Applicant stresses that nowhere does McNair disclose or suggest any system or method that includes a plurality of connection engines distributed among a plurality of subnets and configured to access a server on an IP network. McNair does not include that combination with the mobile office platform device and the database and intelligent routing engine and function as described above. The system of McNair is specifically directed as a security system that controls access to a resource that overcomes the drawback when a hacker tries repeatedly to access the system with trivial variants of easily guessable words or

sequences as noted in the Background of the Invention section at lines 35-45.

FIG. 1 from McNair is reproduced below:

FIG. 1



McNair as indicated in its Summary of the Invention section and reproduced from its FIG. 1 above is directed to a security system that includes a switch, microprocessor and memory and controls access to a resource such that when a user's attempt to access the resource using a password fails, a time interval "t" must elapse before a subsequent attempt at access by that user can be successful, if increased. Thus, McNair is directed to solving a different technical problem as when a hacker repeatedly tries to access a system. McNair solves this technical problem by increasing the increments such that repeated access attempts by hackers or other unauthorized users is discouraged.

McNair is substantially different from the claimed system and method that distinguishes between permanent or persistent transient failures and access a server such as on the internet from a client, for example, using a mobile wireless communications device. Thus, an example embodiment of the claimed system and method may provide a decision that can automatically be made to determine when any reattempts should be made at accessing a server and whether a set period of time should be allowed to pass before reattempting access, or if a different connection engine should be used to initiate communication.

It would be illogical for the system of McNair to use any type of different connection engine as claimed in the instant application because that would give the hacker another chance or "bite at the apple" to try repeatedly to access the server in which he is trying to break into.

Thus, McNair is substantially different from the claimed system and method. This is clearly set forth in the Summary of the Invention section of McNair, which is reproduced below:

> "In accordance with the present invention, a security system controlling access to a resource is arranged to operate such that when a user's attempt to access a resource using a password fails, the time interval "t" that must elapse before a subsequent attempt at access by that user can be successful, is increased. By making the increments increasingly large (illustratively, an exponential function of the number "n" of unsuccessful attempts), repeated access attempts by hackers or other unauthorized users is

> discouraged, because they simply cannot wait the time needed to make a large number of trial and error attempts. On the other hand, valid users, while experiencing a delay prior to access, are nevertheless able to gain access, rather than being completely "locked-out".
>
> In accordance with a feature of this invention, the value of "t" may be decreased in relatively small decrements "d" in response to each of "m" subsequent valid access attempts. By maintaining the value of "t" at a high level after multiple unauthorized access attempts, the authorized user is alerted that there may have been an attempt at unauthorized access. Also, an attempt by a hacker to time access attempts to correspond to valid user actions is frustrated. The approach used in the present invention is thus a better compromise between access control and denial."

As to Bond used by the Examiner to teach a proxy server and applied to claims 9, 31 and 51, Applicant notes that Bond is directed to a voice-over-internet protocol (VoIP) system that accomplishes two-way, three-way, and conference calling between two or more parties and is directed to solving the technical problem of implementing new call features. Bond is nowhere directed to solving the technical problem as addressed with the claimed system and method by distinguishing between permanent or persistent transient failures and accessing a server such as on the internet from a client, for example, using a mobile wireless communications device. One skill in the art would not be motivated to take the security system of McNair and apply it with the VoIP system of Bond to form the claimed system and method.

Fodor as applied to claims 10, 32 and 33 shows POP, IMAP or HTTP mail protocol with a WAP or SMTP used in the load

balancing scheme. Fodor manages mail messages where the mail processing and storage is distributed between multiple mail servers or domains rather than sending mail messages to one primary email server until an over-capacity problem exists as explained in its Summary of the Invention section. Fodor is also directed to load distribution and is not directed to the claimed system and method.

Thus, one skilled in the art would not be motivated to take the security system of McNair and combine it with the load balancing of Fodor to form the claimed system and method.

Applicant contends that the present case is in condition for allowance and respectfully requests that the Examiner issue a Notice of Allowance and Issue Fee Due. If the Examiner has any questions or suggestions for placing this case in condition for allowance, the undersigned attorney would appreciate a telephone call.

Respectfully submitted,

RICHARD K. WARTHER
Reg. No. 32,180
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Phone: 407-841-2330